ANÁLISIS DE LA SEGURIDAD DE SMARTPHONE CON SISTEMA ANDROID

CRISTHIAN JOSÉ MANRIQUE LOZADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ

2019

ANÁLISIS DE LA SEGURIDAD DE SMARTPHONE CON SISTEMA ANDROID

CRISTHIAN JOSE MANRIQUE LOZADA

Monografía

Ing. Martin Camilo Cancelado Ruiz

Director de monografía.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ

2019

DEDICATORIA

A Dios y a mi familia, especialmente a mi esposa Ingrid y a mi abuela, por su apoyo y ayuda fundamental, sin ellas esto no hubiera sido posible.

AGRADECIMIENTOS

A Dios por permitirme cumplir una meta más.

A la universidad UNAD y su cuerpo académico involucrado en este trabajo, ya que gracias a su orientación y correcciones no hubiera sido posible la culminación del mismo.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

Los dispositivos móviles en la actualidad juegan un papel muy importante ya que no solo hacen parte del ocio, entretenimiento, si no de la parte profesional y laboral, esto conlleva que de una u otra manera se esté utilizando de forma constante, al ser así, al estar conectados en la red, al guardar información, al realizar transacciones y demás utilidades brindadas, pueden originar una brecha que puede ser aprovechada por los delincuentes cibernéticos para cometer actos ilícitos, de ahí la importancia de minimizar los riesgos y tener un nivel de seguridad correcto, es de recalcar que al ser Android el principal sistema operativo en dispositivos móviles, es el que presenta mayor número de ataques, así como se trabaja para evitar éste tipo de inconvenientes, también se presenta un desarrollo constante en las modalidades y forma en el actuar de los delincuentes.

Palabras claves: Dispositivos móviles, *Smartphone*, seguridad informática, *malware*, tecnologías de la información y la comunicación.

INTRODUCCIÓN

Inicialmente cuando se hacía referencia a seguridad en cuanto a la parte de informática y sistemas, nos remontábamos solo a equipos de cómputo, pero la evolución tecnológica y la comodidad que representan los dispositivos móviles, los ha convertido en elementos de uso cotidiano.

La seguridad en los dispositivos móviles con sistema operativo Android, es un tema que día a día va tomando más importancia, ya que su notable crecimiento también lo convierte en blanco de ataques de seguridad, debido a que, si se logra generar un ataque, el número de usuarios afectados podría ser mayor.

Considerando los diferentes riesgos de los que pueden ser víctimas los dispositivos móviles, se hace necesario primero identificar las principales amenazas y los efectos que estas puedan tener y posteriormente poder determinar la manera acertada de prevenir cada uno de los ataques.

1. TITULO

ANÁLISIS DE LA SEGURIDAD DE SMARTPHONE CON SISTEMA ANDROID

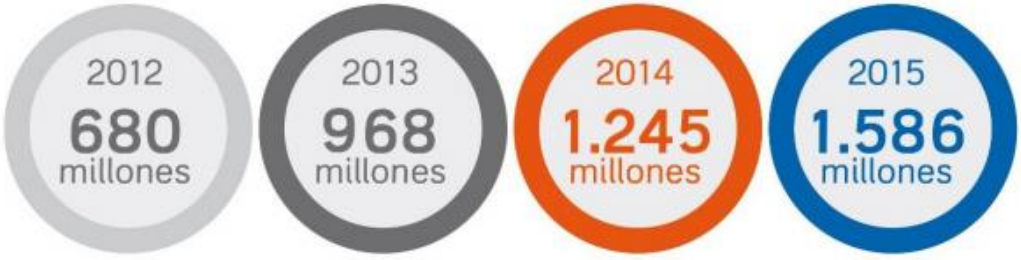
2. FORMULACIÓN DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

Según la revista seguridad de la información[1], un dispositivo móvil es aquel que presenta unas características específicas como su tamaño, que permite ser transportado con facilidad y usado de manera práctica, además que ofrezca una buena capacidad de almacenamiento, conectividad a una red y acceso a un sinfín de aplicaciones; características que lo convierten en una herramienta de uso sencillo que facilitan muchas de las labores de la cotidianidad de las personas.

La evolución de dispositivos móviles en cuanto a sus ventas, ha ido en aumento tal como se puede evidenciar en la figura 1, ya que se pasó de vender 680 millones en el 2012 a 1.586 millones en el 2015.

Figura 1. Evolución de los números de *Smartphone* vendidos en el mundo.



Fuente: Informe Mobile en España y el mundo 2016. Recuperado de http://www.amic.media. 2016

Al observar el grafico anterior se evidencia que la evolución de los *Smartphones* vendidos en el mundo, según el informe mobile en España y el mundo 2016, crece

[1] Revista seguridad de la información. Universidad Nacional Autónoma de México. México. 2017

a pasos agigantados, en el año 2012 la cantidad de smartphones vendidos fue de 680.000.000, con relación a los 1.586.000.000 que se vendieron en el año 2015, un aumento bastante considerable del 116,6% en tres años. Lo anterior coincide con un informe entregado por cisco[2] que sugiere que entre el 2016 y el 2021, habrá 1,5 dispositivos móviles por persona, casi 12.000.000.000 de dispositivos móviles para una población estimada 7.800 millones[3].

La rápida acogida de los dispositivos móviles, el incremento de la cobertura móvil también hace que la demanda de contenido móvil crezca y con él, los ataques, "las descargas de *malware* aumentaron más del 900% con más de 970 descargas por hora, en comparación con 106 anteriores"[4], es así como lo afirma chekpoint en su reporte de seguridad.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son las principales amenazas a la que están expuestos los dispositivos móviles con sistema Android *marshmallow* 6.0?

[2] CISCO. *Informe Cisco VNI Mobil*. http://globalnewsroom.cisco.com. 2016
[3] ONU. http://www.un.org. 2016
[4] CHECKPOINT. Reporte de seguridad 2016. http://pages.checkpoint.com/security-report.html. 2016

3. JUSTIFICACIÓN

El auge que se está presentado con el desarrollo de las aplicaciones para los dispositivos móviles, en el que cada día surgen nuevas herramientas que están al alcance de cualquier persona que cuente con un dispositivo y una conexión a la red; realidad a la que los ciberdelincuentes no son ajenos, utilizando este tipo de desarrollo para realizar ataques o robo de información mediante ciertas aplicaciones que son creadas para estos fines delictivos.

Por lo que es importante tomar ciertas medidas y mecanismos de protección; y algunas veces los usuarios tratan tomar medidas de protección, pero estos ciberdelincuentes siempre están en busca de mejorar sus ataques, por lo que también es importante que las personas estén constantemente actualizando su sistema de protección.

Se eligen los dispositivos móviles con sistema operativo Android, considerando que según StatCounter[5], a abril de 2017, este es el sistema operativo más usado entre computadores, portátiles, tabletas y dispositivos móviles con un 37.93% de uso.

Es necesario conocer la información que existe respecto a esta problemática para identificar las principales amenazas a las que están expuestas los dispositivos móviles con sistema operativo Android y que afecten de manera negativa el funcionamiento de dichos dispositivos, para poder determinar los efectos de estos puedan generar y posteriormente poder aplicar las estrategias más adecuadas para la protección o reducción de estos ataques.

[5] StatCounter, firma gratuita de análisis de datos y estadísticas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Identificar las principales amenazas a la que están expuestos los dispositivos móviles Smartphone con sistema Android

4.2 OBJETIVOS ESPECÍFICOS

Identificar principales ataques que se pueden presentar en las plataformas Android

Identificar los efectos que pueden causar los ataques a dispositivos con sistema operativo Android

Determinar las vulnerabilidades en cuanto a seguridad, que presenta el sistema operativo Android

Determinar los mecanismos que permitan asegurar de forma correcta los dispositivos móviles y sus aplicaciones.

5. **MARCO REFERENCIAL**

5.1 MARCO DEL ESTADO DEL ARTE

Considerando la creciente demanda en el uso de dispositivos móviles que van de la mano con el incremento de los ataques cibernéticos, también se evidencia, dentro de la revisión documental un aumento en los estudios a sobre la seguridad en dispositivos móviles.

Dentro de estos documentos se encontró “Android” el sistema operativo de google para dispositivos móviles” de Malavé, K. y Beaupertuy, J. (2011), este articulo busca dar a conocer la influencia del sistema operativo Android en el mundo de los dispositivos móviles inteligentes. Está investigación es de carácter documental, se realizaron encuestas y entrevistas que buscan emitir conclusiones acerca de las incidencias y ventajas que ofrece este sistema operativo, logrando identificar las características principales que lo convierten en una alternativa para los fabricantes de *Smartphone* y sus usuarios, a pesar del poco tiempo desde su aparición.

Albarracín, Parra y Camargo (2013), en su trabajo “seguridad en dispositivos móviles con sistemas operativos Android y IOS”, presentan un análisis de los aspectos más relevantes de la seguridad de dispositivos móviles con sistema operativo Android y IOS.

Inicia con la descripción de unos antecedentes, luego realiza una conceptualización de los aspectos más relevantes de los sistemas operativos objeto de estudio y finalmente se definen los principales ataques de los que han sido objeto estos sistemas operativos.

Otro de los documentos revisados, “seguridad informática. Aspectos duros y blandos” de Fernández, J. (2013), se define la seguridad informática y establece unos objetivos en esta área, con los que se busca minimizar los riesgos en los ataques a la información.

Estos objetivos incluyen horarios de funcionamiento, restricción a ciertos lugares, perfiles de usuario, autorizaciones y denegaciones y todo lo necesario para contribuir a un buen nivel de seguridad.

El documento “descripción y análisis del modelo de seguridad de Android” de Romano y Luna (2013), realiza una descripción del modelo de seguridad implementado por Android, incluyendo los análisis y crıticas de los trabajos más relevantes hasta el momento y una comparación con el modelo de seguridad de los dispositivos móviles Java.

5.2 MARCO TEÓRICO

5.2.1 Dispositivos móviles. Las características presentes en los diferentes dispositivos tecnológicos han ido evolucionando a través del tiempo, adaptándose a las necesidades de los usuarios, entre los que se destacan los móviles, al tener un menor tamaño, lo que facilita su movilidad. Sin embargo, no es la característica principal de este tipo de dispositivos, el monográfico de seguridad del catálogo STIC considera un dispositivo móvil “aquel que incorpora un sistema operativo diseñado originalmente para dispositivos enfocados a su uso con redes de comunicaciones de telefonía móvil, como Symbian, Android, iOS, Windows Phone, BlackBerry OS, etc.”[6]

[6] Monográficos de Seguridad del Catálogo STIC. Seguridad en dispositivos móviles. Instituto Nacional de Tecnologías de la Comunicación (INTECO). 2012

Android es un sistema operativo para dispositivos móviles “desarrollado y mantenido por Google para *smartphones* y tabletas que ofrece un desarrollo de software libre y tiene herramientas, aplicaciones y emuladores para desarrollar aplicaciones en Java. La plataforma Android aumentó su nivel de ventas del 3.5% en el 2009 a 25.5% en el 2010”.[7]

Anteriormente los sistemas operativos de dispositivos móviles no tenían tanto protagonismo, debido a que las aplicaciones ofrecidas eran más limitadas, ya que estaban más enfocadas hacia el ámbito empresarial, es por esto por lo que la aparición de iOS de Apple y Android de google, marca un hito evolutivo importante, impulsando el desarrollo de aplicaciones útiles en ámbitos cotidianos y de fácil acceso.

Actualmente iOS y Android acaparan una mayor parte en el mercado para este tipo de dispositivos. Sin embargo, no son los únicos ya que coexisten con otras plataformas como Windows Phone- Symbian, de Nokia (anteriormente Windows Mobile) y o BlackBerry OS, que tenían terreno ganado en el ámbito empresarial, pero la competencia de parte de iOS y Android, lo ha dejado bastante afectado.

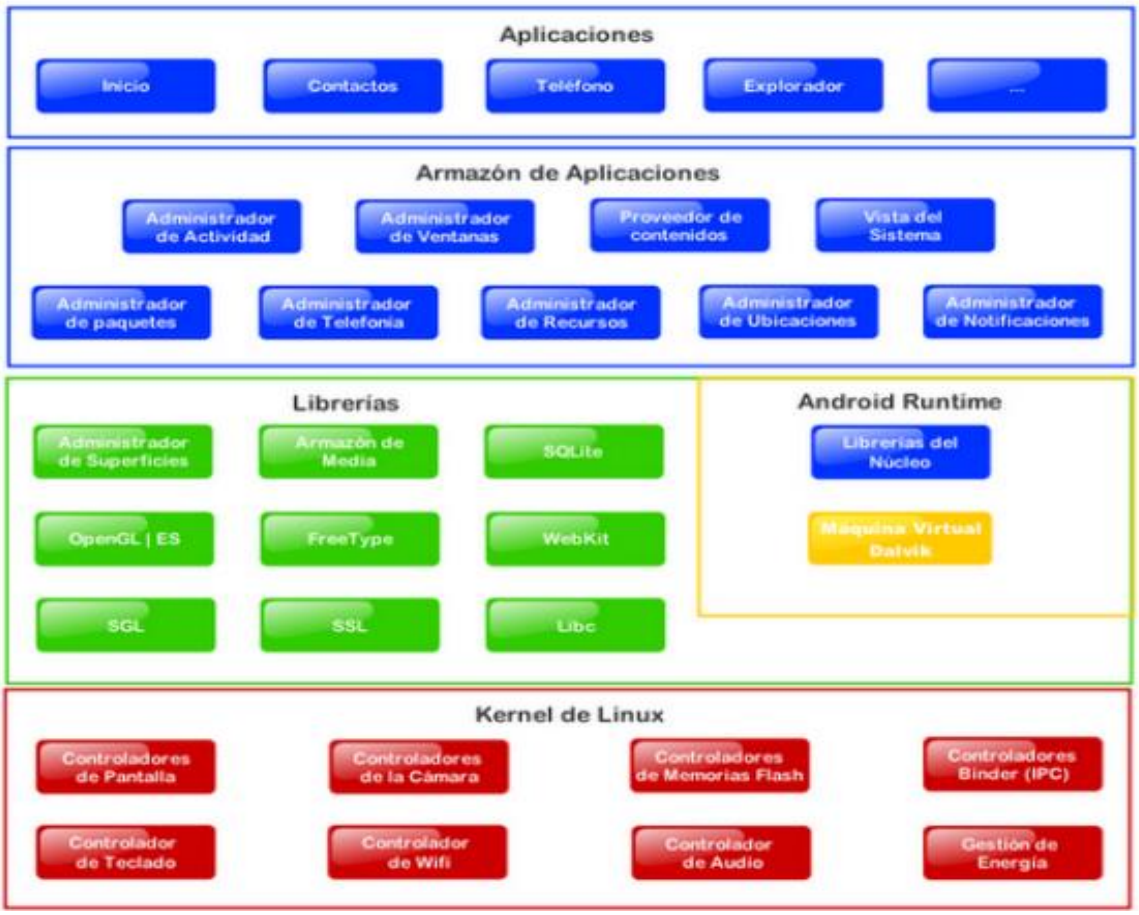
Según *AdroScope*[8], Android se ha convertido en la plataforma más popular para dispositivos móviles, sistema operativo que está basado en Linux, desarrollado por Android inc., Inicialmente solo para dispositivos móviles.

La estructura interna de Android está compuesta por cuatro elementos, como se muestra en la figura 2, aplicaciones, armazón de aplicaciones, librerías y kernel de Linux, funciona a manera de capas, donde cada capa utiliza los servicios de la anterior y ofrece todos los suyos a la siguiente capa.

[7] Gartner. (2010). Gartner Press Releases. Disponible en Internet: http://www.gartner.com/it/ page.jsp?id=1466313

[8] Myeongjin Cho, Ho Jin Lee, Minseong Kim, Seon Wook Kim. AndroScope: un analizador de rendimiento profundo para todas las capas de software de los sistemas basados en Android. Volumen 35, Número 2. 2013.

Figura 2. Arquitectura sistema Andriod



Fuente: Programacion en otras plataformas móviles. Recuperado de: http://ocw.uc3m.es/ingenieria-telematica/software-de-comunicaciones-1/UDs_JME/parte-ii-unidad-4-programacion-en-otras-plataformas-moviles.

5.2.2 Sistema operativo Android. El sistema operativo Android fue creado por Andy Rubin, licenciado en Ciencias de la Computación de la Universidad de Utica, Nueva York, en 2005 cuando google compro Android Inc. Donde el propio Andy supervisaba el desarrollo de este sistema, se inició la evolución, ya que desde ese momento hasta el 2008 cuando se creó la primera versión de Android, google realizo acuerdos con fabricantes de *Smartphone* para desarrollar el primer

dispositivo móvil con sistema Android, dando como resultado que HTC creara el modelo Dream con este sistema el 22 de octubre.

A continuación, se presenta la tabla 1, con las diferentes versiones de Android y sus características.

Tabla 1: Versiones de Android

VERSIONES DE ANDROID			
Versión	**Nombre**	**Fecha**	**Característica**
1.0	Apple Pie	Septiembre de 2008	Esta fue la primera versión de tipo comercial, lanzada en el dispositivo HTC Dream, dentro de sus características se encontraba que poseía pantalla táctil, funcionalidad de navegabilidad y conectividad. En febrero de 2009 se lanzó la actualización 1.1, donde se corrigieron los fallos y errores presentados.
1.5	Cupcake	Abril de 2009	Esta actualización fue la primera versión la cual incluía nombre de postre, iniciando la secuencia que se basaba en orden alfabético. Su principal característica era que disponía de teclado virtual y mejoras en su interfaz.
1.6	Donut	Septiembre de 2009	Esta versión incorpora la búsqueda rápida, en cuanto a su contenido, ya que no solo se basa en la búsqueda de la web, sino que también dispone se acceso a contactos, aplicaciones y demás apartados.

Tabla 1 (Continuación)

Versión	Nombre	Fecha	Característica
2.0	Eclair	Octubre de 2009	Su lanzamiento principal se dio en enero de 2010, con el Nexus One, donde se dio inicio a la serie de teléfonos de google. Otra característica fue la incorporación de google maps en esta versión.
2.2	Froyo	Mayo de 2010	Sus paneles de inicio se ampliaron de 3 a 5, como también accesos directos, se realizaron mejoras en la parte de videos y capacidad de memoria. Se agregó la opción de disponer de contraseña o pin en la pantalla desbloqueo, los usuarios disponían de pin como de patrón para desbloquear sus teléfonos.
2.3	Gingerbread	Diciembre de 2010	Esta versión se lanzó con el dispositivo Nexus S, google se apoyó de Samsung para esta creación. La pantalla era su atractivo ya que era curva, se mejoró el rendimiento de su batería, además informaba al usuario que aplicación estaba consumiendo la batería del equipo.
3.0	Honeycomb	Febrero de 2011	Esta actualización era exclusiva para Tablet, el primer dispositivo fue el Motorola Xoom, no era apta para Smartphone, al ser así, elimino los botones físicos. En cuanto a su interfaz también se generaron cambios ya que estaba dedica a dispositivos de pantalla de mayor tamaño.

Tabla 1 (continuación)

Versión	Nombre	Fecha	Característica
4.0	Ice Cream Sandwich	Octubre de 2011	Era soportado por Tablet y por Smartphone, se lanzó con el dispositivo Samsung Galaxy Nexus. A esta actualización se le incorporo el bloqueo facial, como también el análisis de datos el cual informa que aplicación consume más datos.
4.1	Jelly Bean	Julio de 2012	El primer dispositivo en utilizar esta actualización fue la tablet Nexus, se enfocó principalmente en mejorar la funcionalidad y la interfaz del usuario.
4.3	Jelly Bean (Michel)	Julio de 2013	Con esta versión se lanzó la segunda generación de los Nexus 7, dentro de sus características se destaca la conectividad 4G LTE y mejoras en la seguridad.
4.4	KitKat	Noviembre de 2013	Se lanzó con los dispositivos Nexus 5 de google y LG, se implementó la impresión desde los dispositivos vía wifi, se mejora el rendimiento del sistema.
5.0	Lollipop	Noviembre de 2014	Se caracteriza principalmente por el diseño, debido a sus nuevos colores e imágenes de ayuda de borde a borde, se destaca la iluminación, las sombras de tipo realista, todo esto facilita y hace más amigable el uso de los dispositivos.

Tabla 1 (continuación)

Versión	Nombre	Fecha	Característica
6.0	Marshmallow	Octubre de 2015	Con esta actualización se introducen ciertas funcionalidades que consolidan a Android como un sistema solido, principiante la función la cual permite que al cambiar de dispositivo o restaurarlo de fábrica conserva las aplicaciones y datos descargados anteriormente.
7.0	Nougat	Agosto de 2016	Se lanzó con los dispositivos Nexus 6, 5X, 6P, Nexus Player, Pixel C y Android One, se mejora el uso de la batería, las actualizaciones tanto del sistema como de las aplicaciones son más rápidas, lo que conlleva que el sistema sea más eficiente y rápido.
8.0	Oreo	Agosto de 2017	Dentro de sus funciones se destacan la mejoría de la gestión de las notificaciones, sección de texto inteligente y autorelleno de texto nativo.
9.0	Pie	Agosto de 2018	A la fecha de la realización de esta monografía, Pie es última versión desarrollada, posee sistema de navegación por deslizamiento, función de batería adaptativa, que da prioridad a la aplicación que se usan con más frecuencia. Es de recalcar que con cada versión se realizan mejoras y se corrigen errores de las versiones anteriores.

Fuente: el autor.

La información proporcionada por google, (citado por Tapia 2018) acerca del porcentaje de instalación de las versiones de Android, se evidencia que la más popular a septiembre de 2018 es Marshmallow 6.0 con 21.6%, como se puede observar en la siguiente figura:

Figura 1. Cantidad de instalación de las versiones de Android.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.1%
4.2.x		17	1.6%
4.3		18	0.5%
4.4	KitKat	19	7.8%
5.0	Lollipop	21	3.6%
5.1		22	14.7%
6.0	Marshmallow	23	21.6%
7.0	Nougat	24	19.0%
7.1		25	10.3%
8.0	Oreo	26	13.4%
8.1		27	5.8%

Fuente: unocero recuperado de: https://www.unocero.com/software/android-versiones-mas-usadas-smartphones/

Considerando la información anterior, para efectos de la presente monografía, se determinó como objeto de estudio el análisis de la seguridad de *Smartphone* con sistema Android versión Marshmallow 6.0.

5.2.3 Seguridad Informática. En la actualidad es un tema el cual ha ido creciendo de forma considerable, debido a varios factores, entre los que se destacan el auge de dispositivos que se encuentran sincronizados con toda la información personal del usuario, esta da pie para que cada día se generen constantes amenazas de robo o pérdida de información, esto en el ámbito personal, pero en el ámbito empresarial o grandes organizaciones.

La Seguridad informática tiene como objetivo proteger, cuidar y salvaguardar todo tipo de información y la estructura tecnológica que conforman un sistema, sea complejo o sencillo; también nos permite conocer posibles fallas o riesgos que estén latentes a fin de evitar daños, o si se presentan que se registre el menor traumatismo posible.

Seguridad informática Según José Fernández[9], es un gran área que se enfoca en la protección de la estructura tecnológica y todo lo relacionado, haciendo énfasis en la información, todo esto se da por medio de estándares, protocolos, métodos y demás herramientas las cuales permiten minimizar los posibles riesgos que se pueden llegar a presentar, ya sea a través de *hardware* y *software*, la tarea principal de la seguridad informática es asegurar todos los recursos del sistema, que se encuentre lo más seguro posible, además que la información sea utilizada de manera correcta, que sea manipulada por las personas que tengan acreditación para realizar esas funciones.

La seguridad en dispositivos móviles, es un tema que poco a poco tomo gran importancia en la actualidad, como lo indica José Manuel Ortega[10], la era de la tecnología móvil es un aspecto a tener en cuenta, debido al constante tráfico de navegación, como al momento de realizar cualquier tipo de descarga, por esta razón se deben de reducir al máximo los riesgos que se pueden llegar a presentar,

[9] Fernández, José. Seguridad en Informática. Aspectos Duros y Blandos. México. 2014
[10] José Manuel Ortega. Escuela Politécnica Superior.

actualmente Android y iOS son las plataforma más utilizadas, en el presente se nota un dominio de Android, hay un factor que diferencia estos dos tipos de sistemas, Android se basa código abierto mientras iOS dispone de una plataforma más cerrada, los malware también atacan este tipo de dispositivos, de un modo similar a los computadores, ya que se instala sin consentimiento, con la intención por lo general de robar información para fines delictivos y lucrativos.

Según IDC Quarterly Mobile Phone Tracker[11] las empresas de telefonía móvil vendieron el primer trimestre del 2017 un total de 344,3 millones de dispositivos móviles, estas cifras demuestran lo grande y lo importante que es este sector, aun cuando se comparan con cifras anteriores y se evidencia una reducción, la demanda de teléfono inteligentes sigue siendo fuerte.

Las comunicaciones móviles han tenido gran avance en relación con las comunicaciones fijas, tal como lo indica Montiel. J.[12] ya que se toma como complemento de estas, esto se ve reflejado en países desarrollados como Japón y USA, en donde el incremento es notorio en relación con las comunicaciones fijas donde se presenta un decremento, otro ejemplo claro es que, en América Latina, los usuarios de comunicaciones móviles presentan un aumento del 90%.

Los dispositivos móviles como lo indica César Tardáguila Moro[13], son aquellos microordenadores, que poseen un tamaño adecuado para ser trasportado por una persona inclusive en un bolsillo, como también de disponer de una batería lo suficientemente autónoma, el primer dispositivo móvil fue la Newton, creado por Apple en 1993.

[11] IDC analyze the future. 2017. https://www.idc.com/promo/smartphone-market-share/os
[12] Montiel Pérez, Jesús. et al. Computación móvil. (en línea). Ingeniare. Revista chilena de ingeniería. 2012. Disponible desde internet en https://dx.doi.org/10.4067/S0718-3052012000300001
[13] Tardáguila Mor, Cesar. Dispositivos Móviles y Multimedia. (en línea). Repositorio Institucional: Universitat Oberta de Catalunya (UOC). 2012. Disponible desde internet en http://www.temoa.info/es/node/145900.

En la actualidad las personas prefieren tener como plataforma de comunicación los teléfonos celulares, debido a su tamaño y a su funcionalidad que cada día tiende a mejorar, como lo indica Enrique V. Carrera[14] esta preferencia también origina ciertas amenazas que cada día toman diferentes formas, pero con un fin común, que es atacar la seguridad de los usuarios mediante estos dispositivos, otro punto a tener en cuenta en cuanto a la seguridad de este tipo de dispositivos, es que permite fácil conexiones a redes externas y esto conlleva a que los riesgos aumente de gran manera.

Android, es el sistema operativo más usado actualmente, es desarrollado por Google, está basado en Linux, su principal objetivo es enfocarse en teléfonos inteligentes, tables y otros dispositivos, según Basterra - Bertea - Borello - Castillo - Venturi[15] las ventajas de Android son: posee código abierto, su núcleo basado en el *Kernel* de Linux, adaptable a muchas pantallas y resoluciones, Utiliza *SQLite* para el almacenamiento de datos, entre otras, su base principal se da por medio del *Kernel* totalmente basado en Linux, es el que permite el correcto funcionamiento del sistema operativo.

Cuando se instala Android, no solo se dispone de un sistema operativo, adicionalmente se cuenta con un conjunto de aplicaciones especiales tal como lo indica Agustín Romano Carlos Luna[16], estas con libretas de contacto, reloj, entre otras las cuales permiten el funcionamiento del sistema, también dispone de un *middleware* que brinda librerías y servicios del sistema, una característica con la cual dispone el sistema operativo Android es, que las aplicación ya sean principal o creada por cualquier desarrollador, se puede instalar sin ningún problema en el dispositivo, para así poder acceder a los recurso del dispositivo, eso sí dependiendo permisos dados.

[14] Carrera, Enrique. El Costo de la Seguridad en Dispositivos Móviles. (en línea) Universidad San Francisco de Quito. 2017. Disponible desde internet en http://sapyc.espe.edu.ec/evcarrera/papers/ictitc10.pdf
[15] Android OS Documentation Release 0.1 2017. Creative Commons AtribuciónCompartirIgual 3.0 Unported.
[16] Descripción y análisis del modelo de seguridad de Android. Agustín Romano Carlos Luna

Al ser Android uno de los sistemas operativos más usados en dispositivos móviles, presenta mayor número de ataques, esto se ve reflejado en un estudio realizado por Nokia NES (NetGuard Endpoint Security) ya que en el 2016 el 81% de dispositivos que sufrieron ataques estaban bajo la plataforma de Android, esto quiere decir que un 85% de los *smartphones* se están viendo afectados por este tipo de incidentes relacionados con ataques de malware.

"De ese porcentaje, el 81% corresponde a dispositivos Android, mientras que el 4% restante pertenece a terminales de Apple. Por otro lado, el informe de Nokia avisa de que en octubre de 2016 se alcanzó el récord de aumento de tasa de infección, siendo éste un 1,35%, la cifra más alta desde 2012 (año en el que comenzó el estudio)"[17].

Ser el más popular puede traer grandes consecuencias, tal como le está ocurriendo al sistema operativo Android, todo se origina al ser uno de los más usados, debido a que es más factible para un atacante o delincuente asechar y sacar provecho si afecta una plataforma con millones de usuarios, no hay que desconocer el esfuerzo que se está dando con cada actualización para mitigar al máximo todos estos problemas que presenta la plataforma en el ámbito de la seguridad, no hay que dejar a un lado que parte de la seguridad en los dispositivos móviles y cualquier tipo dispositivo depende del uso que cada persona le dé, ya que al navegar en redes no protegidas, no seguras, realizar descargar sin verificar el sitio, el creador u origen, pueden llegar afectar el sistema o en el peor de los casos verse afectado por un ataque informático, que pueden llegar a robar información como fotos, archivos o tomar información bancaria y financiera, sabiendo lo que esto puede llegar acarrear.

[17] XACATACAN. Los ataques de malware en dispositivos móviles. 2015. Disponible en internet en https://www.xatakandroid.com/seguridad/los-ataques-de-malware-en-dispositivos-moviles-aumentan-y-android-es-el-principal-objetivo-segun-nokia.

5.3 MARCO CONCEPTUAL

5.3.1 Android. Sistema operativo y una plataforma software, basado en Linux para dispositivos móviles.[18]Permite programar aplicaciones en *Dalvik*, una variación de Java; debido a que es de código libre, permite la creación de aplicaciones e incluso la modificación del mismo sistema operativo.

Este sistema operativo ha ido evolucionando de manera apresurada, al igual que los teléfonos móviles, desde la versión 1.0 “Apple pie” en el 2008, hasta la 9.0 “pie” en el 2018.

5.3.2 Aplicaciones**.** Tipo de *software* que funciona como un conjunto de herramientas diseñado para realizar tareas y trabajos específicos en tu computador.[19] Estas aplicaciones permiten desarrollar tareas de cualquier tipo, puede ser educativas, profesionales, de acceso a servicios, ocio, entre otras.

Las aplicaciones al ser residentes en los dispositivos móviles debido a su diseño de programación compilado, aportan unas ventajas como:

- Un acceso más rápido y sencillo a la información necesaria sin necesidad de los datos de autenticación en cada acceso.
- Un almacenamiento de datos personales que, a priori, es de una manera segura.
- Una gran versatilidad en cuanto a su utilización o aplicación práctica.
- La atribución de funcionalidades específicas.
- Mejorar la capacidad de conectividad y disponibilidad de servicios y productos (usuario-usuario, usuario-proveedor de servicios, etc.).[20]

[18] Baez, Manuel. Et al. Introducción a Android. E.M.E. Editorial. 2012
[19] GCFAprende libre. (en línea). 2016. Disponible desde internet en https://www.gcfaprendelibre.org/tecnologia/curso/informatica_basica/explora_mac_os_x/4.do
[20] American Dialect. «“App” voted 2010 word of the year by the American Dialect Society (UPDATED)» (en inglés). Consultado el 19 de mayo de 2013.

5.3.3 Dispositivos tecnológicos. Objeto asociado de ciencia y tecnología, usado por el hombre para optimizar tareas cotidianas.[21] En la actualidad, los dispositivos tecnológicos están presentes en casi todos los espacios cotidianos y responden a múltiples tareas desde académicas hasta recreativas.

5.3.4 IOS. Por sus siglas en inglés (*iPhone Operating System*) Sistema operativo móvil para dispositivos fabricados por Apple. Restringe el uso de dispositivos a los de su propia fabricación; en la parte tecnológica no permite tecnologías como *Java* o *Flash*, lo que hace que los componentes de algunas páginas no sean accesibles desde sus navegadores y otras aplicaciones.

5.3.5 *Java.* Lenguaje de programación de alto nivel para escribir diversos programas.[22] Fue diseñado por la compañía *Sun Microsystems* con el objetivo de crear programas pequeños, confiables, trasportables y veloces.

5.3.6 *Linux*. Sistema operativo de libre distribución. Este software proporciona cuatro libertades:

- Libertad de ejecución.
- Libertad de estudio.
- Libertad para compartir y distribuir.
- Libertad de mejorar.

[21] Fernández-González, M., & Torres-Gil, A. (2014). Los dispositivos tecnológicos cotidianos en libros de texto. Presencia y análisis de las exposiciones. Revista Eureka sobre Enseñanza y Divulgación de las Ciencias, 11 (3), 290-302.
[22] Ceballos, Francisco. Java 2. Curso de Programación. 4ª edición. 2010

5.3.7 *Middleware*. Conjunto de servicios comúnmente utilizadas por muchas aplicaciones para funcionar bien dentro de un ambiente interconectado. [23] Este software se sitúa entre un sistema operativo y las aplicaciones que se ejecutan en él. Básicamente, funciona como una capa de traducción oculta para permitir la comunicación y la administración de datos en aplicaciones distribuidas. A veces, se le denomina "*plumbing*" (tuberías), porque conecta dos aplicaciones para que se puedan pasar fácilmente datos y bases de datos por una "canalización". El uso de middleware permite a los usuarios hacer solicitudes como el envío de formularios en un explorador web o permitir que un servidor web devuelva páginas web dinámicas en función del perfil de un usuario.[24]

5.3.8 *Malware*. Contracción de malicious software, indica todo aquel software que afecta la computadora, son utilizados con múltiples fines como extraer contraseñas, información personal o evitar que los usuarios accedan a sus dispositivos.[25]

5.3.9 Seguridad informática**.** Purificación Aguilera define la seguridad informática como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener un sistema seguro y confiable.[26]

5.3.10 Sistema operativo. Conjunto de programas diseñados para la ejecución de varias tareas. Este software se encarga de la coordinación y dirección de todas las

[23] La organización IETF (Internet Engineering Task Force). 1997.
[24] https://azure.microsoft.com/es-es/overview/what-is-middleware/
[25] https://www.avast.com/es-es/c-malware
[26] Aguilera, Purificación. Seguridad informática. 2010

aplicaciones que utiliza el usuario. Los sistemas operativos más utilizados son *Windows, Linux, OS/2* y *DOS*[27].

Un sistema operativo cuenta con tres componentes esenciales:

- Sistema de archivos.
- Interpretación de comandos.
- El núcleo que permite el funcionamiento de los elementos básicos del software.

5.3.11 *Smartphone*. También llamados celulares inteligentes, incorporan mucha más capacidad y de procesos.

5.3.12 *Softwar*e libre. Hace referencia a programa libre, en la publicación software libre en educación, aclara que el *free software* (termino tomado del inglés), no traduce específicamente "gratis", sino que este término está más encaminado hacia la libertad de expresión que permiten este tipo de software, ya que "el propietario de los derechos sobre el software libre garantiza a los usuarios, mediante una licencia, una serie de libertades que no otorga el propietario del software privativo, que se reserva numerosos derechos en base a la legislación sobre propiedad intelectual (por ejemplo, no permite el acceso al código fuente o no permite ninguna modificación y su subsecuente distribución)"[28].

5.3.13 *Sqlite*. Daniel Ponsoda, en su introducción a SQLite, la define como "una librería compacta y autocontenida de código abierto y distribuida bajo dominio

[27] https://concepto.de/sistema-operativo/#ixzz62ea4sSYk
[28] Lolanda, Jordi. Software libre en educación. Depto. de Educación Universitat Jaume I Castellón (España) v.2. 2007.

público que implementa un gestor de bases de datos SQL embebido, sin configuración y transaccional."[29]

5.3.14 *Windows phone*. Es un sistema operativo móvil desarrollado por Microsoft, que integra algunos servicios propios como: Skype, one drive y Xbox Live.

5.4 MARCO LEGAL

La 1273 de 2009, creada para modificar el código penal y crea un bien jurídico "de la protección de la información y de los datos", con el fin de preservar la seguridad en las tecnologías de la información y las telecomunicaciones. Realiza una revisión de los diferentes delitos que afectan la integridad, confidencialidad y disponibilidad de la ciberinformación.

Esta ley en su primer capítulo hace referencia a los atentados contra la confidencialidad, integridad y disposición de los datos informáticos, el capítulo II habla de los atentados informáticos y otras infracciones.

La ley 1341 de 2009 por la cual "definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones" , esta ley tiene por objeto determinar el marco general para la formulación de políticas públicas en el sector de las tecnologías de la información y las comunicaciones, desde el punto de organización, competencia, inversión, cobertura y calidad del servicio, así como también la protección al usuario, inspección, control y vigilancia.

[29] Ponsoda, Daniel. Introducción a SQLite. Creative Commons. 2008.

El documento del consejo nacional de política económica y social CONPES 3854 de 2016 enfocado a la política nacional de seguridad digital, se crea a raíz del creciente uso de las tecnologías de la información y la comunicación en Colombia, lo que indiscutiblemente genera diversos riesgos, que el ministerio afirma, deben estudiarse constantemente

Esta política de ciberseguridad y ciberdefensa, hasta el momento está enfocada en defensa del país, el cibercrimen y como elemento importante incluido en este nuevo documento es la integración de la gestión del riesgo con el fin de poder identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

6. ANÁLISIS DE LA SEGURIDAD DE SMARTPHONE CON SISTEMA ANDROID *MARSHMALLOW* 6.0

La versión 6.0 del sistema operativo de Android, denominada *Marshmalow,* disponible a partir de octubre de 2015, posee ventajas en cuanto a la seguridad de acceso al dispositivo, con la incorporación del lector de huellas para bloquear el teléfono y también de aplicaciones. Otra de las ventajas se presenta en el tratamiento de permisos que las aplicaciones requieren, es decir que se pueden consultar los permisos de cada aplicación y en caso de no estar de acuerdo, el usuario puede denegarlos. También se incluye dentro de la información, la fecha del ultimo parche de seguridad, ya que cada mes se actualiza el SO, con el fin de corregir los agujeros de seguridad que se presenten.

Sin embargo, *Kaspersky Lab*, ha descubierto la modificación de un troyano bancario con la capacidad de eludir los elementos de seguridad implementadas por el SO, logrando adquirir derechos sobre las aplicaciones, efectuar llamadas, enviar y leer mensajes, pero su función más peligrosa es la de robar datos de la tarjeta de crédito y credenciales bancarias.

El *malware* se vale de un sistema de superposición de ventanas que engaña a los usuarios, especialmente a través de mensajes de correo electrónico que contienen enlaces maliciosos. Una vez logra instalarse en el dispositivo, adquiere los permisos necesarios para tomar control del dispositivo.

En lo referente a las aplicaciones Android, *Marshmalow* permite tener acceso a ellas ya que brinda información y configuración de las mismas, dando la opción de escribir sobre otras aplicaciones, de determinar las aplicaciones preestablecidas y realizar ajustes al sistema.

Los niéveles de los parches de seguridad se pueden determinar en esta versión, ya que Google y otros fabricantes se comprometieron a lanzar dichas actualizaciones de forma mensual, para así disminuir el riesgo de posibles vulnerabilidades masivas, el usuario así sabrá que tan actualizado esta su equipo, cuando se trató este tema, la gran mayoría de fabricantes apostó por esta opción, pero algunos no lo tomaron tan enserio.

Otro punto a destacar en cuanto a la seguridad en la versión Android *Marshmalow*, fue la del cifrado por defecto de la memoria interna, en este tema Google tomo medidas obligando a los fabricantes a cifrar por defecto todo, esto para minimizar la fuga de información ya sea por ataques como *tapjacking*, que consiste en la captura de los toques que el usuario da en la pantalla, o en caso de pérdida o robo del dispositivo móvil.

En cuanto a la autenticación en esta versión, los fabricantes están en la obligación de establecer un sistema de seguridad temporal que inhabilite el acceso cuando se presenten ataques de fuerza bruta, antes de esta versión los fabricantes no estaban en la obligación de realizar dicha implementación, este sistema se ve reflejado cuando se ingresa el patrón de desbloqueo o la huella incorrecta y al intento número cinco el dispositivo se bloquea por 30 segundos.

En un estudio realizado por parte de Google, en la actualización que publicó para desarrolladores el 10 de octubre de 2018, indico que la versión más utilizada era la Android 6.0 *Marshmalow,* con un 21.3%, seguida de su predecesora la *Nougat* 7.0 con un 18.1% en tercer lugar la versión Lollipop 5.1 con un 14.4%, lo que indica que las mejoras que presento la *Marshmalow,* demostró su eficiencia y funcionalidad que se ve reflejado en su gran avance en materia de seguridad.

Por su parte *Lollipop* 5.0 que fue la antecesora de *Marshmalow* 6.0, presento ciertas características dentro de las que se destacan la utilización de la tecnología

NFC, el cual permite migrar los datos de las cuentas de otros dispositivos, otro aspecto a destacar dentro de esta versión la es opción que da posibilidad de restablecer la configuración de fábrica y a la ves borrar todos los datos que se encuentren almacenamos en el dispositivo de una manera remota, siendo muy útil en caso de robo o pérdida del móvil.

Un punto a destacar de la versión *Lollipop* 5.1 en materia de seguridad, es la incorporación del módulo de protección SELinux, la función principal de este módulo es evitar el *malware* que se puede llegar a presentar.

Otro tipo de protección que brindó, es referente a la vinculación del dispositivo mediante cuentas de Google, ya que, si presenta un evento infortunado como robo o pérdida, se debe de ingresar las credenciales de acceso de dicha cuanta para utilizar el dispositivo.

Un tipo de ataque que se presentó en Android, es el *malware* bancario, tan solo en 2015 se presentaron alrededor de 1,6 millones de paquetes de instalación que contenían algún tipo malicioso, por lo general un Troyano diseñado para infiltrarse en el dispositivo y su principal objetivo es acceder al dispositivo para así tener todos los datos de inicio de sesión y contraseñas bancarias, después de obtener esta información, se enviaba a un servidor de mando previamente configurado por el atacante. Con el solo hecho de realizar transferencia de dinero o pagos de facturas, se tenían los datos de interés para el atacante, el tercer trimestre de 2015 el *malware* bancario fue la amenaza que presento más rápido crecimiento en su actuar.

El *malware* bancario, se ha presentado también por medio de aplicaciones, que se encuentran en la tienda oficial Google *Play*, un ejemplo de ello es la aplicación *Cleand Droid*, la cual mejora el rendimiento del equipo, actualmente se encuentra en la tienda, pero al ser reportada al equipo de seguridad de Google, se restringió

su descarga en algunos países; otras aplicaciones de este tipo, proporcionan la posibilidad de saber que usuarios visitaron el perfil, una vez instaladas, se indicaba que se debía de activar los servicios de accesibilidad, de esta manera solicitaban a los usuarios ingresar las credenciales a ciertas aplicaciones legitimas, de tipo bancario, financiero, de compras en línea entre otras, todo esto mediante una interfaz falsa generada por la aplicación maliciosa, para así obtener este tipo de información.

El *Ransomware* no ha estado alejado de las plataformas móviles, en el 2015 se presentaron casos de este tipo, que, al momento de verse afectado el dispositivo, el atacante tiene acceso a la información y por lo general solicita rescate por dicha información ya sea en bitcoins o en dinero, rastrear a estos delincuentes fue complicado ya que ellos se valieron de la herramienta TOR para no ser rastreados con facilidad.

Un claro ejemplo de *Ransomware* es *DoubleLocker* que dentro de su actuar, esta la posibilidad de bloquear el dispositivo por completo mediante el cambio del pin, como también cifrar la información que se encuentre almacenada en el mismo, para así cobrar por esta, o por el acceso al dispositivo, la forma de distribución de este tipo de ataque se originó mediante una versión falsa de *Adobe Flash Player*, que se subian a sitios web comprometidos, una vez instalado, se ejecutaba en segundo plano sin que el usuario se percatara de lo sucedido, por esta razón se recomienda realizar copia de información con frecuencia para que en caso tal de verse afectado, se pueda restablecer la configuración del mismo y con el *Backup* de información esta estaría a salvo.

Otro tipo de ataque que se presentó en mayo del 2015 fue a raíz de los *Spyware* móvil, este tipo de programa se instala en los dispositivos y vigila toda la actividad registrada, desde ubicación, nombres de usuario, contraseñas, en ocasiones este

tipo de ataque no es visible para la victima ya que ejecuta en un segundo plano sin que se puede llegar a sospechar de él.

Un ataque que se presentó también en el 2015 fue el de Troyanos de SMS, ya que para esa fecha los mensajes de texto tenían más popularidad, todo se daba por medio de un mensaje de texto, el cual permitía acceder a información confidencial y posteriormente se envía por medio de mensaje de texto al delincuente.

Un troyano SMS conocido fue el *FakeInst*, su diseño era ser una aplicación diseñada para ver paginas web pornográficas, al iniciar la instalación, el usuario aceptaba los términos y condiciones que por lo general estaban en ruso, donde se aceptaba el envío de mensajes, con esto el atacante obtenía toda la información del dispositivo, como el control total de todos los mensajes de texto, se podían borrar, enviar y demás acciones, al tener este control, se realizan suscripciones de contenidos premium, lo cual generaba costos que eran cargados al usuario.

Android.Bankbot.65.Origin, era el nombre del Troyano que se originó en Rusia, tomo la apariencia de la aplicación *Sberbank Online* oficial, su función era de banco móvil, ya que con los datos de los usuarios se presentaron robos millonarios, todo esto es por qué no se percibía diferencia entre las aplicaciones y el usuario creía que estaba en la oficial.

También las molestas ventanas emergentes han estado presentes en los dispositivos móviles, denominadas *Adware*, ya que por medio de estas se crea un código malicioso el cual con solo dar clic realiza la descarga e instalación de dicha aplicación que permite tomar cierta información útil para el atacante.

En 2011 Symantec realizó un estudio el cual identifico las principales amenazas que estaban presentes en los dispositivos móviles, tal como se indica en la figura 4, dentro de las amenazas que se destacan están:

- Ataques basados en la web y en redes
- *Software* malicioso
- Ataques de ingeniería social
- Abuso de disponibilidad de servicios y recursos
- Pérdida de datos por acción maliciosa y no intencionada
- Ataques sobre la integridad de los datos del dispositivo

Figura 4. Principales amenazas hacia dispositivos móviles.

Fuente: symantec recuperado de: https://www.symantec.com/content/es/mx/enterprise/images/theme/mobiletrends/mobile-device-infograph-es.jpg

Como se puede evidenciar los tipos de amenazas siempre han estado presente, la diferencia es que, con el paso de los días, se toman medidas las cuales evitan situaciones de riesgo que están presente o se puedan llegar a presentar, en este punto es donde los ciberdelincuentes no se quedan atrás y buscan la forma de romper las medidas de seguridad que se implementan.

Tabla 2: CVE Vulnerabilidades 2015

Posición	Nombre Del Sistema Operativo	Numero de Vulnerabilidades
1	Mac OS X	444
2	Iphone Os	387
4	Opensuse	269
5	Ubuntu Linux	264
26	**Android**	**125**

Fuente: El autor.

El número de vulnerabilidades abiertas que presento Android en 2015 según CVE (*Common Vulnerabilities and Exposures)* fue de 125 ubicándose en el número 26, dentro de las principales vulnerabilidades se destacan las qué permitían al atacante ejecutar un código malicioso donde se veía comprometida toda la información que se encontraba en el dispositivo, así como la misma protección del sistema, todo esto era posible ya que por lo general el código se ocultaba en archivos de tipo multimedia.

Otro tipo de vulnerabilidad que se presento fue denomina CVE-2015-1528, la cual permitía al atacante tener control del dispositivo y de la información mediante aplicaciones creadas para tal fin las cuales se ejecutaban en un segundo plano sin que el usuario se percatara de lo ocurrido.

Tabla 3: CVE Vulnerabilidades 2016

Posición	Nombre Del Sistema Operativo	Numero de Vulnerabilidades
1	**Android**	525
2	Debian Linux	334
3	Ubuntu Linux	286

Fuente: El autor.

En el listado publicado por la de la CVE (*Common Vulnerabilities and Exposures)* del año 2016, Android paso a tener 523 vulnerabilidades ubicándolo en el primer lugar.

Uno de los ataques que revelo este listado en el 2016 se presentó en los dispositivos móviles Samsung Galaxy S4 a S7, mediante mensajes *WAP Push SMS*, ya que permitía la ejecución de código malicioso, el cual daba acceso al atacante a toda la información almacenada como los datos y configuración del sistema.

Mediante el acceso a redes Wifi, los atacantes accedían a los dispositivos, a través de aplicaciones diseñas, lo cual permitían como sucede en la mayoría de ataques acceder a la información y obtener control del equipo.

Tabla 4. CVE Vulnerabilidades 2017

Posición	Nombre Del Sistema Operativo	Numero de Vulnerabilidades
1	**Android**	843
2	Linux Kernel	454
3	Iphone Os	387
4	Debian Linux	367

Fuente: El autor.

En el listado emitido en el año 2017 por la CVE (*Common Vulnerabilities and Exposures)*, Android seguía ocupando el primer lugar con un total de 843 vulnerabilidades.

Debido al auge que se presenta en el uso de dispositivos móviles con el sistema operativo Android, también se puede observar que los niveles de ataques se han ido incrementado año tras año, ya que utilizan desde mensajes de texto, archivos de cualquier tipo, ubicación de *GPS* y demás aplicaciones o herramientas que permitan llegar a un objetivo, que siempre por lo general es el mismo obtener información y accesos a los dispositivos.

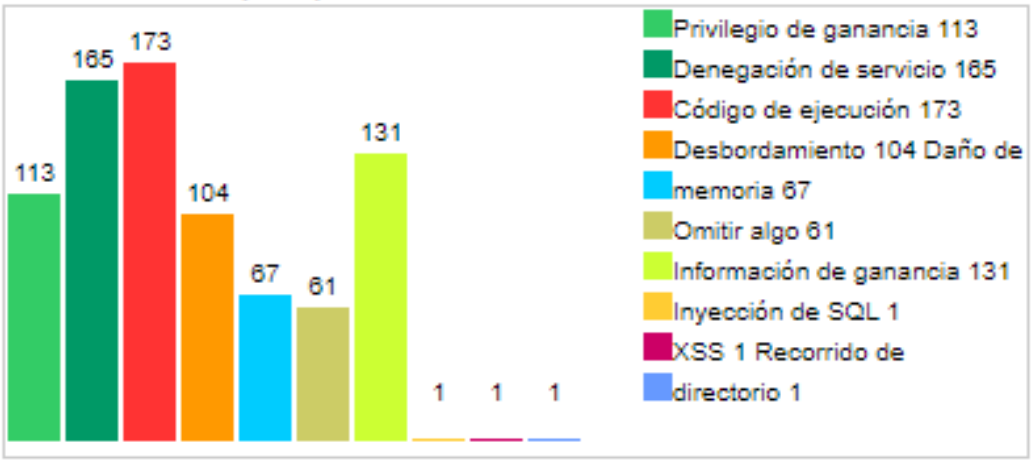
En el 2018 la CVE (*Common Vulnerabilities and Exposures)* indico que Android tuvo 611 vulnerabilidades ubicándose en un tercer lugar; de ahí la importancia de tener los dispositivos móviles actualizados en esencial todo lo relacionado con los parches de seguridad ya que estos no permiten disminuir los riegos que se pueden llegar a presentar.

Con relación al listado de la CVE (*Common Vulnerabilities and Exposures)*, lo importante no es número de vulnerabilidades que se presenten, si no detectarlas y buscar una solución oportuna y acorde a sus niveles de requerimientos.

6.1 VULNERABILIDADES PRESENTADAS POR LA VERSIÓN ANDROID 6.0

En cuanto al tipo de vulnerabilidades que presenta la versión 6.0 de Android, la CVE (*Common Vulnerabilities and Exposures*), expone una serie de vulnerabilidades identificadas por tipo, tal como se indica en la figura 5.

Figura 5. Vulnerabilidades por tipo en Android 6.0



Fuente: https://www.cvedetails.com/version/187788/Google-Android-6.0.html?fbclid=IwAR3eVqIy53NrsAbIvXts100ZRRjFa9xNTLF9BMZZnI_5pDSDm43tOhi_MIs

Según el listado de vulnerabilidades publicadas por la CVE (*Common Vulnerabilities and Exposures*) la versión 6.0 de Android presentó vulnerabilidades de diversos tipos, dentro de las que predominan, las de código de ejecución con un total de 173, en segundo lugar, la denegación de servicio con un total de 165 ataques y en tercer lugar las de información de ganancia con un total de 131 ataques.

Un tipo de ataque que utiliza el código de Ejecución (vulnerabilidad: CVE-2017-0588) es el que se genera mediante un archivo especifico que está diseñado para afectar la memoria durante el procesamiento de datos y de archivos multimedia, esta vulnerabilidad se presentó en las versiones Android desde la versión 4.4, hasta 7.1.

En cuanto a uno de los ataques de denegación de Servicio (vulnerabilidad: CVE-2015-6608), consiste en permitir al atacante vía remota ejecutar un código o causar una denegación de servicio, todo esto mediante un archivo multimedia diseñado para tal fin, también identificados como errores internos 19779574,

23680780, 23876444 y 23658148, esta vulnerabilidad afecto las versiones Android 5.1 y 6.0

Finalmente, uno de los ataques de información de Ganancia (vulnerabilidad: CVE-2015-6621), se da por medio de una aplicación diseñada, que permite a los atacantes obtener privilegios y credenciales de acceso, esta vulnerabilidad también se identifica como error interno 23909438, se presentó en las versiones Android 5.0, 5.1 y 6.0.

6.2 MECANISMOS DE PROTECCIÓN

En cuanto a los mecanismo o niveles de protección que se puedan dar para asegurar los dispositivos móviles con sistema Android, se inicia desde la seguridad que presta *Google Play Store*, ya que con el paso del tiempo las condiciones para publicar aplicaciones en la tienda se han ido incrementando, todo esto se vio reflejado a partir de la versión 4.3 de Android, donde se mejoró el respaldo de claves que permiten brindar más seguridad, adicionalmente los desarrolladores o empresas que deseen realizar publicaciones en la tienda deben de cumplir ciertos criterios en las políticas de seguridad.

La protección de estos dispositivos inicia desde la seguridad que se implemente en el acceso, a través del uso y correcta configuración del bloqueo de pantalla, como lo son el Patrón de Bloqueo, Código Pin y Bloqueo por huella, al tenerlos activados, se minimizan los riesgos ya que cualquier persona no tendrá acceso de una forma fácil.

Al realizar las actualizaciones correspondientes tanto al propio sistema como a las aplicaciones, al tenerlas actualizadas los riesgos disminuyen ya que cada actualización por lo general corrige fallas presentes y a futuro que se puedan dar, lo mismo sucede con los parches de seguridad, dado que su función es corregir

problemas de seguridad que se estén presentado, lo que tiene que ver con las aplicaciones, Android ya dispone de la opción de configuración de permisos de las aplicaciones, donde se puede ver que permiso y acceso tienen cada una de ellas.

Otro punto a tener en cuenta son las conexiones de tipo Wifi, ya que al conectarse a una red pública no confiable, con el solo hecho de aceptar de la conexión, la persona que brinda esta red puede tener acceso a la información del dispositivo, por esta razón si es necesario conectarse a este tipo de redes, lo que se recomienda es que no realice cualquier tipo de transacción que solicite datos de gran importancia como lo son los de tipo bancarios.

Con la creación de *Bouncer,* la aplicación que permite asignar permisos temporales o denegarlos a las apps instaladas, se dio más afectividad en las aplicaciones publicadas, ya que su finalidad es analizar todas las aplicaciones para detectar posibles códigos maliciosos y de ser encontrado algún tipo de *malware*, troyano o *spyware*, se procederá a eliminar y a generar una notificación, por esta razón se deben de realizar descarga de sitios y tiendas oficiales, como lo seria en este caso *Google Play Store*, ya que de alguna manera brindan cierta seguridad al realizar las descargas.

Por otro lado, si se presenta sospecha de alguna aplicación, se debe de validar los permisos que tiene activados, por lo general las aplicaciones maliciosas no implementan ningún tipo de protección para realizar la desinstalación, es decir que si sospecha de una aplicación lo mejor es realizar la desinstalación.

Básicamente para que el dispositivo móvil este seguro se deben cumplir las tres capas de seguridad las cuales son:

- La protección del dispositivo: en este caso el móvil debe de estar configurado parar realizar borrado de forma remota si se llega a presentar pérdida o robo del mismo.
- Protección de datos: se debe evitar la interacción con datos críticos, como lo son los personales y bancarios, en redes publicas y con aplicaciones poco confiables.
- Seguridad de gestión de aplicaciones: en cuanto a las aplicaciones que estén instaladas, deben de estar actualizadas y con los permisos necesarios para el correcto funcionamiento de las mismas.

7. CONCLUSIONES

La revisión documental que se efectuó para la elaboración de la presente monografía permitió realizar un análisis a la seguridad en los dispositivos móviles sistema operativo Android, especialmente de la versión 6.0.

Según la CVE (*Common Vulnerabilities and Exposures),* Android, se ubica en el puesto número 26 dentro de la cantidad de vulnerabilidades detectadas en los sistemas operativos de dispositivos móviles. Dentro de los principales ataques detectados se encuentra uno de código malicioso, oculto en archivos multimedia, que permite al atacante tener control de toda la información del dispositivo e incluso el de la protección del sistema. Otro ataque que tiene objetivos similares al anterior, se ejecuta en segundo plano a través de aplicaciones, por lo que el usuario no se da cuenta de lo que sucede.

Kaspersky Lab, advierte de un troyano bancario con la capacidad de evitar los elementos de seguridad del sistema operativo, logrando tomar control de todo el dispositivo, realizando llamadas, enviar y leer mensajes, pero lo más delicado es su función de obtener datos de inicio de sesión y contraseñas bancarias. Algunos cifran la información almacenada para luego cobrar rescate por esta, ya sea por medio de bitcoin o dinero.

Los ataques a Android, así como a todos los sistemas operativos, están en constante crecimiento, Symantec en 2011, identifico las principales amenazas presentadas a la fecha: software malicioso, ataques de ingeniería social, abuso de disponibilidad de servicios y recursos, perdida de datos por acción maliciosa y ataques cobre la integridad de los datos del dispositivo.

En cuanto a las vulnerabilidades que presenta el sistema operativo Android, es importante tener en cuenta que, aunque constantemente se establezcan nuevos mecanismos de protección, los ciberdelincuentes continuamente buscan la manera de poder atacar dichos mecanismos o sistemas.

Asegurar de forma correcta los dispositivos y las aplicaciones, empieza desde la protección que se le dé al mismo para el acceso, es decir a través del uso de bloqueo de pantalla, código PIN, patrón de bloqueo y bloqueo por huella, entre otros elementos de seguridad que pueda presentar el equipo.

Otro de los elementos claves en cuanto a seguridad, son las conexiones wifi, ya que aceptar o vincularse a una red no confiable, podría darle acceso a la información del dispositivo a la persona que maneje la red; algo similar puede suceder al descargar aplicaciones de sitios no oficiales, por lo que es recomendable el uso de la tienda de google para la descarga de cualquier *app.*

Sin embargo, uno de los elementos más importantes de seguridad, es la realización de cada una de las actualizaciones correspondientes tanto al sistema, como a las aplicaciones, ya que de esta manera se pueden corregir las fallas de seguridad que se estén presentando.

Considerando la importancia que han tomado este tipo de dispositivos en la cotidianidad de la mayoría de las personas, es sumamente importante que los usuarios conozcan los riesgos a los que pueden exponerse y así tomar las medidas necesarias de protección.

Analizando las vulnerabilidades más comunes, se puede evidenciar que el usuario es la mayor debilidad en el sistema de seguridad, ya que la falta de conocimiento lo lleva a conceder accesos a aplicaciones mal intencionadas, otra de las fallas es no tener precaución con sus datos personales.

Los creadores de software tipo malware constantemente mejoran sus tácticas de ataque, razón para que los usuarios, también evolucionen en sus estrategias de protección pues la mayor parte de los ataques se dan por descuidos de las personas.

Para fortalecer la seguridad y reducir el margen de ataques, es importante que los desarrolladores estén constantemente mejorando las buenas prácticas de programación, pero también es importante que los usuarios descarguen las aplicaciones desde los sitios autorizados y que se informen sobre el contenido de las mismas.

REFERENCIAS BIBLIOGRÁFICAS

AGUILERA López, Purificación. Seguridad informática, 1st ed., vol. 1. Editex, 2010.

ALBARRACIN, Juan Carlos. PARRA Camargo, Leidy Maribel. Y CAMAGO Vega, Juan Jose. SEGURIDAD EN DISPOSITIVOS MÓVILES CON SISTEMAS OPERATIVOS ANDROID Y IOS. Tecnología, Investigación y Academia. 2013. Disponible http://revistas.udistrital.edu.co/ojs/index.php/tia/article/view/4312

BAZ, Alonso. FERREIRA, Irene. ÁLVAREZ, María. y GARCÍA, Rosana. Dispositivos móviles. Ingeniería de Telecomunicación Universidad de Oviedo. 2009.

CANDELA, Santiago. GARCÍA, Carmelo Rubén. QUESADA, Alexis. SANTANA, Francisco José. y SANTOS, José Miguel. Fundamentos de sistemas operativos: teoría y ejercicios resueltos. Editorial Paraninfo, 2007.

CARACTERÍSTICAS DEL SISTEMA OPERATIVO ANDROID (1995). En: http://www.samsung.com/co/article/android-2-2- os-explained/

CARRERA, Enrique. El Costo de la Seguridad en Dispositivos Moviles. Universidad San Francisco de Quito. 2010

CISCO. Informe Cisco VNI Mobile. En: *http://globalnewsroom.cisco.com. 2016*

DOMINGO Prieto, Marc. Seguridad en dispositivos móviles. Openlibra. 2013

ESTUDIO SOBRE SEGURIDAD EN DISPOSITIVOS MÓVILES Y SMARTPHONES. INTECO 2012. En: https://www.red.es/redes/sites/redes/files/estudio_moviles_3c11.pdf

FERNANDEZ, Jose. Seguridad en Informática. Aspectos Duros y Blandos. 2013

GIRONES, Jesús Tomas. El gran libro de Android. Segunda edición. México: Alfaomega, 2012. 403p.

MONTIEL Pérez, Jesús Yaljá. HERNÁNDEZ Rubio, Erika, y LÓPEZ Bonilla, José Luis. Computación móvil. Revista Chilena de Ingeniería. En: https://www.redalyc.org/articulo.oa?id=77225004001

ONU. http://www.un.org. 2016

Reporte de seguridad 2016. http://pages.checkpoint.com/security-report.html. 2016

ORTEGA, José Manuel. Escuela Politécnica Superior. Disponible en: https://www.idc.com/promo/smartphone-market-share/os

TARDÁGUILA Moro, Cesar. Dispositivos Móviles y Multimedia. Tecnologias y comunicación multimedia. 2009.

ANEXOS

Anexo A. RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. INFORMACIÓN GENERAL DE LA PROPUESTA DE MONOGRAFÍA – DOCUMENTO RAE

Fecha**:**	Octubre 22 de 2019
Título de la propuesta**:**	Análisis de la seguridad de smartphone con sistema Android

INTEGRANTE Cristhian José Manrique Lozada

Nombre del estudiante: Cristhian Manrique Lozada					
Identificado con	C.C. X	C.E	Otro	Número: 93236941	
Programa Académico		Especialización en Seguridad Informática		Correo Electrónico	Kiliman11@hotmail.com
No. de Créditos Aprobados del plan de estudios:				Promedio Acumulado:	
Dirección residencia:					Municipio / Departamento Ibagué - Tolima
Teléfono / Celular 310 3634463				Zona Sur	CEAD Ibagué

2. DATOS ESPECÍFICOS DE LA MONOGRAFÍA	
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Escuela:	Escuela de Ciencias Básicas, Tecnología e Ingeniería
Descriptores palabras claves:	Análisis, Seguridad, Dispositivos Móviles
Nombre del asesor (Docente) del trabajo	

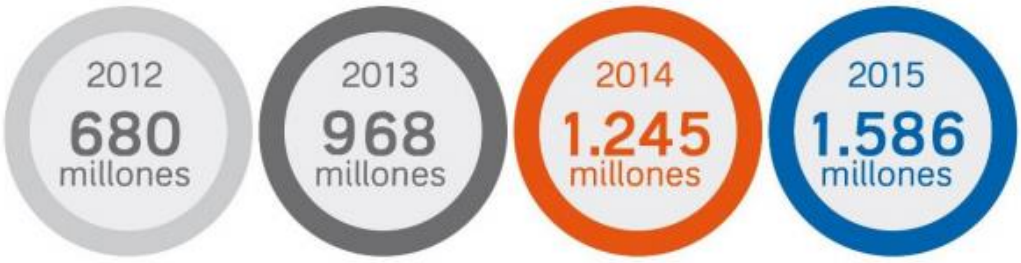
3. RESUMEN (200 palabras máximo)

Los dispositivos móviles en la actualidad juegan un papel muy importante ya que no solo hacen parte del ocio, entretenimiento, si no de la parte profesional y laboral, esto conlleva que de una u otra manera se esté utilizando de forma constante, al ser así, al estar conectados en la red, al guardar información, al realizar transacciones y demás utilidades brindadas, pueden originar una brecha la cual es aprovechada por los delincuentes cibernéticos para cometer actos ilícitos, de ahí la importancia de minimizar los riesgos y tener un nivel de seguridad correcto, es de recalcar que al ser Android el principal sistema operativo en dispositivos móviles, es el que presenta mayor número de ataques, así como se trabaja para evitar éste tipo de inconvenientes, también se presenta un desarrollo constante en las modalidades y forma en el actuar de los delincuentes.

4. PLANTEAMIENTO DEL PROBLEMA (500 palabras máximo)

La evolución de dispositivos móviles en cuanto a sus ventas, ha ido en aumento tal como se puede evidenciar en la figura 1, ya que se pasó de vender 680 millones en el 2012 a 1.586 millones en el 2015.

Figura 2. Evolución de los números de *Smartphone* vendidos en el mundo.



Fuente: Informe Mobile en España y el mundo 2016. Recuperado de http://www.amic.media. 2016

Al observar el grafico anterior se evidencia que la evolución de los *Smartphones* vendidos en el mundo, según el informe mobile en España y el mundo 2016, crece a pasos agigantados, en el año 2012 la cantidad de smartphones vendidos fue de 680.000.000, con relación a los 1.586.000.000 que se vendieron en el año 2015, un aumento bastante considerable del 116,6% en tres años. Lo anterior coincide con un informe entregado por cisco[30] que sugiere que entre el 2016 y el 2021, habrá 1,5 dispositivos móviles por persona, casi 12.000.000.000 de dispositivos móviles para una población estimada 7.800 millones[31].

La rápida acogida de los dispositivos móviles, el incremento de la cobertura móvil también hace que la demanda de contenido móvil crezca y con él, los ataques, "las descargas de *malware* aumentaron más del 900% con más de 970 descargas por hora, en comparación con 106 anteriores"[32], es así como lo afirma *chekpoint* en su reporte de seguridad.

FORMULACIÓN DEL PROBLEMA

¿Cuáles son las principales amenazas a la que están expuestos los dispositivos móviles con sistema Android *marshmallow* 6?0?

5. JUSTIFICACIÓN (500 palabras máximo)

El auge que se está presentado con el desarrollo de las aplicaciones para los dispositivos móviles, en el que cada día surgen nuevas herramientas que están al alcance de cualquier persona que cuente con un dispositivo y una conexión a la red; realidad a la que los ciberdelincuentes no son ajenos, utilizando este tipo de desarrollo para realizar ataques o robo de información mediante ciertas aplicaciones que son creadas para estos fines delictivos.

Por lo que es importante tomar ciertas medidas y mecanismos de protección; y algunas veces los usuarios tratan tomar medidas de protección, pero estos ciberdelincuentes siempre están en busca de mejorar sus ataques, por

[30] CISCO. *Informe Cisco VNI Mobil*. http://globalnewsroom.cisco.com. 2016
[31] ONU. http://www.un.org. 2016
[32] CHECKPOINT. Reporte de seguridad 2016. http://pages.checkpoint.com/security-report.html. 2016

lo que también es importante que las personas estén constantemente actualizando su sistema de protección.

Se eligen los dispositivos móviles con sistema operativo Android, considerando que según StatCounter[33], a abril de 2017, este es el sistema operativo más usado entre computadores, portátiles, tabletas y dispositivos móviles con un 37.93% de uso.

Es necesario conocer la información que existe respecto a esta problemática para identificar las principales amenazas a las que están expuestas los dispositivos móviles con sistema operativo Android y que afecten de manera negativa el funcionamiento de dichos dispositivos, para poder determinar los efectos de estos puedan generar y posteriormente poder aplicar las estrategias más adecuadas para la protección o reducción de estos ataques.

6. OBJETIVO GENERAL

Identificar las principales amenazas a la que están expuestos los dispositivos móviles con sistema Android

7. OBJETIVOS ESPECÍFICOS

Identificar principales ataques que se pueden presentar en las plataformas Android.

Identificar los efectos que pueden causar los ataques a dispositivos con sistema operativo Android.

Determinar las vulnerabilidades en cuanto a seguridad, que presenta el sistema operativo Android.

Determinar los mecanismos que permitan asegurar de forma correcta los dispositivos móviles y sus aplicaciones.

8. MARCO CONCEPTUAL Y TEÓRICO (sin límite de palabras)

MARCO DEL ESTADO DEL ARTE

Considerando la creciente demanda en el uso de dispositivos móviles que van de la mano con el incremento de los ataques cibernéticos, también se evidencia, dentro de la revisión documental un aumento en los estudios a sobre la seguridad en dispositivos móviles.

Dentro de estos documentos se encontró “Android” el sistema operativo de google para dispositivos móviles” de Malavé, K. y Beaupertuy, J. (2011), este articulo busca dar a conocer la influencia del sistema operativo Android en el mundo de los dispositivos móviles inteligentes. Está investigación es de carácter documental, se realizaron encuestas y entrevistas que buscan emitir conclusiones acerca de las incidencias y ventajas que ofrece este sistema operativo, logrando identificar las características principales que lo convierten en una alternativa para los fabricantes de *Smartphone* y sus usuarios, a pesar del poco tiempo desde su aparición.

MARCO TEÓRICO

Dispositivos móviles. Las características presentes en los diferentes dispositivos tecnológicos han ido

[33] StatCounter, firma gratuita de análisis de datos y estadísticas.

evolucionando a través del tiempo, adaptándose a las necesidades de los usuarios, entre los que se destacan los móviles, al tener un menor tamaño, lo que facilita su movilidad. Sin embargo, no es la característica principal de este tipo de dispositivos, el monográfico de seguridad del catálogo STIC considera un dispositivo móvil "aquel que incorpora un sistema operativo diseñado originalmente para dispositivos enfocados a su uso con redes de comunicaciones de telefonía móvil, como Symbian, Android, iOS, Windows Phone, BlackBerry OS, etc."[34]

Sistema operativo Android. El sistema operativo Android fue creado por Andy Rubin, licenciado en Ciencias de la Computación de la Universidad de Utica, Nueva York, en 2005 cuando google compro Android Inc. Donde el propio Andy supervisaba el desarrollo de este sistema, se inició la evolución, ya que desde ese momento hasta el 2008 cuando se creó la primera versión de Android, google realizo acuerdos con fabricantes de *Smartphone* para desarrollar el primer dispositivo móvil con sistema Android, dando como resultado que HTC creara el modelo Dream con este sistema el 22 de octubre.

Android, es el sistema operativo más usado actualmente, es desarrollado por Google, está basado en Linux, su principal objetivo es enfocarse en teléfonos inteligentes, tables y otros dispositivos, según Basterra - Bertea - Borello - Castillo - Venturi[35] las ventajas de Android son: posee código abierto, su núcleo basado en el *Kernel* de Linux, adaptable a muchas pantallas y resoluciones, Utiliza *SQLite* para el almacenamiento de datos, entre otras, su base principal se da por medio del *Kernel* totalmente basado en Linux, es el que permite el correcto funcionamiento del sistema operativo.

MARCO CONCEPTUAL

Android. Sistema operativo y una plataforma software, basado en Linux para dispositivos móviles.[36]Permite programar aplicaciones en *Dalvik*, una variación de Java; debido a que es de código libre, permite la creación de aplicaciones e incluso la modificación del mismo sistema operativo.

Este sistema operativo ha ido evolucionando de manera apresurada, al igual que los teléfonos móviles, desde la versión 1.0 "Apple pie" en el 2008, hasta la 9.0 "pie" en el 2018.

Dispositivos tecnológicos. Objeto asociado de ciencia y tecnología, usado por el hombre para optimizar tareas cotidianas.[37] En la actualidad, los dispositivos tecnológicos están presentes en casi todos los espacios cotidianos y responden a múltiples tareas desde académicas hasta recreativas.

***Sqlite*.** Daniel Ponsoda, en su introducción a SQLite, la define como "una librería compacta y autocontenida de código abierto y distribuida bajo dominio público que implementa un gestor de bases de datos SQL embebido, sin configuración y transaccional."[38]

[34] Monográficos de Seguridad del Catálogo STIC. Seguridad en dispositivos móviles. Instituto Nacional de Tecnologías de la Comunicación (INTECO). 2012
[35] Android OS Documentation Release 0.1 2017. Creative Commons AtribuciónCompartirIgual 3.0 Unported.
[36] Baez, Manuel. Et al. Introducción a Android. E.M.E. Editorial. 2012
[37] Fernández-González, M., & Torres-Gil, A. (2014). Los dispositivos tecnológicos cotidianos en libros de texto. Presencia y análisis de las exposiciones. Revista Eureka sobre Enseñanza y Divulgación de las Ciencias, 11 (3), 290-302.
[38] Ponsoda, Daniel. Introducción a SQLite. Creative Commons. 2008.